CLAIMS

What is Claimed is:

1. A method of providing security a network, said method comprising:

a) detecting a first packet being broadcast in said network, said first packet having associated with it an address that identifies an untrusted device in said network; and

b) in response to said detection, broadcasting a signal to cause said first packet to be corrupted, wherein said first packet is ignored by devices in said network.

2. The method of Claim 1, further comprising:

c) re-broadcasting said signal in response to said first packet being detected again.

3. The method of Claim 1, further comprising:

c) determining that a collision was not caused by broadcasting said signal; and

d) re-broadcasting said signal according to a predetermined protocol in anticipation of further packets being broadcast from said untrusted device.

4. The method of Claim 3, wherein d) comprises:

d1) continually broadcasting said signal, wherein a collision will be caused with any packet broadcast.

5. The method of Claim 1, wherein said devices in said network are substantially compliant with the IEEE 802.3 specification.

6. The method of Claim 1, wherein said address is a physical address for said untrusted device.

7. The method of Claim 1, wherein said address is a Medium Access Control (MAC) address.

8. The method of Claim 1, wherein said address is a source Medium Access Control (MAC) address of said first packet.

9. The method of Claim 1, wherein said address is a destination Medium Access Control (MAC) address of said first packet.

10. The method of Claim 1, wherein said network is an Ethernet.

11. A device for providing security in a network, said device comprising:

memory to store a list of addresses;

detection logic for detecting a first packet that is considered a security risk, said detection based on comparing said list of addresses with an address in said first packet;

logic to transmit a second packet while said first packet is being broadcast, wherein said device is operable to cause a collision between said first packet and said second packet.

12. The device of Claim 11 wherein said list of addresses comprises trusted addresses.

13. The device of Claim 11 wherein said list of addresses comprises untrusted addresses.

14. The device of Claim 11 wherein said detection logic is further for comparing a physical address in said first packet with said list of addresses.

15. The device of Claim 14 wherein said physical address is a medium control access (MAC) destination address.

16. The device of Claim 14 wherein said physical address is a medium control access (MAC) source address.

17. The device of Claim 11 wherein said device further comprises logic operable to transmit a warning message if a packet having an untrusted address is detected.

18. The device of Claim 11 wherein said device is selected from the group comprising: a router, a switch, and a network interface card (NIC).

19. A method for providing security in a segment of a network, said method comprising:

a) determining that a first packet broadcast in said segment is associated with an untrusted node; and

b) broadcasting a second packet to cause a collision between said first packet and said second packet, wherein nodes in said network ignore said first packet.

20. The method of Claim 19, wherein a) comprises:

a1) reading an address in said first packet, said first packet received at a first node; and

a2) determining that said address is on a list stored on said first node, said list comprising unauthorized addresses, wherein said first packet is determined to be associated with said untrusted node if said address is on said list.

21. The method of Claim 20 further comprising:

c) adding to said list of unauthorized addresses an unauthorized address.

22. The method of Claim 19, wherein a) comprises:

a1) reading an address in said first packet, said first packet received at a first node, said list comprising authorized addresses; and

a2) determining that said address is on a list stored on said first node, wherein said first packet is determined to be associated with said untrusted node if said address is not on said list.

23. The method of Claim 22 further comprising:

c) adding to a list of authorized addresses an authorized address.

24. The method of Claim 19, further comprising:

c) determining that a third packet broadcast in said segment is associated with said untrusted node; and

d) broadcasting a fourth packet to cause a collision between a said third packet and said fourth packet, wherein nodes in said segment ignore said third packet.